DMP:NJM

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

| | |
|---|---|
| IN THE MATTER OF THE SEARCH OF A BLACK IPHONE 7+, FCCID BCG-E3087A1C579C-E3087A, CURRENTLY IN THE CUSTODY OF THE NEW YORK CITY POLICE DEPARTMENT | **TO BE FILED UNDER SEAL**<br><br>APPLICATION FOR A SEARCH WARRANT FOR AN ELECTRONIC DEVICE<br><br>Case No. 18-MJ-197 (RML) |

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

I, WILLIAM J. PUSKAS, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Task Force Officer ("TFO") with the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF"). I have been a TFO since 2014 and have served in the New York City Police Department ("NYPD") for over 21 years. I have been involved in the investigation of numerous cases involving robberies and firearms offenses, including searches and forensic review of phones and other electronic devices. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1951 and 924(c) have been committed, are being committed, and will be committed (the "TARGET OFFENSES"). There is also probable cause to search the information described in Attachment A for evidence and instrumentalities of these crimes as described in Attachment B.

## IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is a black iPhone 7+, FCCID BCG-E3087A1C579C-E3087A (the "Device"), currently in the custody of the NYPD.

6. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

## PROBABLE CAUSE[1]

7. On or about March 5, 2018, two male perpetrators approached a gas station location at 8930 Avenue D, Brooklyn, New York, while one of the employees of the gas station ("Employee-1") was pumping gas into the vehicle of an off-duty NYPD officer (the "Officer"). Another employee of the gas station ("Employee-2") was in the "island" booth at the gas station.

8. One of the perpetrators ("Robber-1") approached Employee-1 and stated, in sum and substance and in part, "don't fucking move."

---

[1] The descriptions of events that took place on or about March 5, 2018, are based on interviews with eyewitnesses. This summary reflects those interviews in sum and substance and in part.

9. The other perpetrator, later identified as William Simon, approached Employee-2, held a firearm by the side of his leg, and demanded, in sum and substance and in part, that Employee-2 give him money. Employee-2 responded, in sum and substance and in part, that he did not have money. Simon patted down Employee-2, then attempted to strike Employee-2 with his hand.

10. At or around the time that Simon was attempting to strike Employee-2, Robber-1 told Simon, in sum and substance and in part, that it was time to "bounce."

11. During the attempted robbery, the Officer fired at the perpetrators, hitting Simon. Robber-1 fled the scene.

12. Simon was pronounced dead shortly thereafter. A silver firearm was recovered from the ground underneath Simon's legs, and the Device was recovered from Simon's personal effects and clothing brought with Simon to the hospital.

13. Based on my training and experience, I know that individuals who commit crimes with others, including robberies, commonly use mobile devices such as cellular telephones to communicate with co-conspirators through voice calls, text messages, emails, and other means. I further know that individuals who steal property or possess stolen property commonly use mobile devices to arrange to conceal, sell, transport, or dispose of the stolen property.

14. In particular, the facts in this case suggest coordination between the robbers. At least two people were involved in the attempted robbery. It is highly probable that some or all of these people communicated with each other by cellular telephone in order to arrange the approach of and/or the departure from the location, division of proceeds from the robbery, and acquisition of weapons.

15. The Device is currently in the lawful possession of the NYPD, having been recovered from Simon's personal effects and clothing. Therefore, while the NYPD might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

16. The Device is currently located in the Eastern District of New York. I know that the Device has been stored in a manner that will ensure that its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the NYPD.

**TECHNICAL TERMS**

17. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing

dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the Device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System (generally abbreviated "GPS") to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets,

and presentations. PDAs may also include GPS technology for determining the location of the devices.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

18. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, PDA, and GPS navigation device. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the Device.

## ELECTRONIC STORAGE AND FORENSIC ANALYSIS

19. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

20. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little

or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

21. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how

the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

22. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

23. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

## CONCLUSION

24. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

## REQUEST FOR SEALING

25. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online. Premature disclosure of the contents of this affidavit and related documents may have a

significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

S/ WILLIAM J. PUSKAS

William J. Puskas
Task Force Officer
Bureau of Alcohol, Tobacco, Firearms and Explosives

Subscribed and sworn to before me
on March 8, 2018

S/ ROBERT M. LEVY

THE HONORABLE ROBERT M. LEVY
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

**ATTACHMENT A**

The property to be searched is a black iPhone 7+, FCCID BCG-E3087A1C579C-E3087A, currently in the custody of the New York City Police Department.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

**ATTACHMENT B**

1. All records on the Device described in Attachment A that relate to violations of **Title 18, United States Code, Sections 1951(a) and 924(c),** and involve **William Simon** since January 1, 2018, including:

a. any information regarding coordination prior to the March 5, 2018 attempted robbery, and any other robbery in which Simon may have participated, with regards to selection of a target, logistical planning for arrival at, departure from, and division of proceeds of the robbery;

b. any evidence regarding gas stations or other commercial establishments, including evidence that Simon or co-conspirators were casing possible robbery sites;

c. any correspondence with co-conspirators;

d. any evidence relating to social media sites used by, or containing photographs of, Simon or his co-conspirators;

e. any photographs, videos, or other media recordings of Simon or his co-conspirators constituting evidence of the crime, including depictions of the perpetrators in clothing similar to the clothing worn during the robbery conspiracy, depictions of the perpetrators with firearms, and depictions of the perpetrators with proceeds of one or more robberies;

f. types, amounts, and prices of guns purchased or some as well as dates and places of specific transactions;

g. any information related to sources of guns (including names, addresses, phone numbers, or any other identifying information);

h. any information related to the division of robbery proceeds (including names, addresses, phone numbers, or any other identifying information);

i. any information recording Simon's schedule or travel from January 1, 2018, to the present;

j. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.